DATE(S) ISSUED:

4/12/2011

SUBJECT:

Cumulative Security Update of ActiveX Kill Bits (MS11-027)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft products that utilize ActiveX controls. Exploiting these vulnerabilities could allow an attacker to take complete control of an affected system. ActiveX controls are small programs or animations that are downloaded or embedded in web pages which will typically enhance functionality and user experience. Exploitation may occur if a user visits a web page, or opens an HTML-formatted email which is specifically crafted to take advantage of one or more of these vulnerabilities. Successful exploitation of any of these vulnerabilities could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

• Windows XP

• Windows Vista

• Windows 7

• Windows Server 2003

• Windows Server 2008

RISK:

Government:

• Large and medium government entities: **High**

• Small government entities: **High**

Businesses:

• Large and medium business entities: **High**

• Small business entities: **High**

Home users: High

DESCRIPTION:

Three vulnerabilities have been discovered in Microsoft products that utilize ActiveX controls. These vulnerabilities could allow an attacker to take complete control of an affected system.

Microsoft Internet Explorer 8 Developer Tools Vulnerability

The first vulnerability exists in the Internet Explorer 8 Developer Tools ActiveX control. Exploitation may occur if a user visits a web page, or opens an HTML-formatted email containing a specifically crafted ActiveX control.

Microsoft WMITools ActiveX Control Vulnerability

The second vulnerability exists in one of the WMITools ActiveX controls. Exploitation may occur if a user visits a web page, or opens an HTML-formatted email containing a specifically crafted ActiveX control.

Microsoft Windows Messenger ActiveX Control Vulnerability

The third vulnerability exists in the Windows Messenger ActiveX control. Exploitation may occur if a user visits a web page, or opens an HTML-formatted email containing a specifically crafted ActiveX control.

Third Party ActiveX Kill Bits

Third party Active X controls for Oracle, CA and IBM have also been included in this security update to prevent the following ActiveX controls from being run in Internet Explorer:

The Oracle ActiveX control is for Java Deployment Toolkit. Additional information about this vulnerability can be found at http://www.oracle.com/technetwork/topics/security/alert-cve-2010-0886-094541.html.

The CA ActiveX control relates to WebScan.

The IBM ActiveX control pertains to the "Rational Suite License ActiveX Control."

RECOMMENDATIONS:

The following actions should be taken:

• Apply the security update provided by Microsoft to vulnerable systems immediately after appropriate testing.

• Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

• Configure email-clients to preview messages in plain-text format, rather than RTF or HTML format.

• Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Microsoft:

http://www.microsoft.com/technet/security/bulletin/ms11-027.mspx

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0811

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3973

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1243

Security Focus:

http://www.securityfocus.com/bid/45546

http://www.securityfocus.com/bid/40490
http://www.securityfocus.com/bid/47197